ANALYSIS OF IPv6 THROUGH IMPLEMENTATION OF TRANSITION TECHNOLOGIES AND SECURITY ATTACKS

Wael Alzaid and Biju Issac
School of Computing, Teesside University, UK

ABSTRACT

IPv6 provides more address space, improved address design, and greater security than IPv4. Different transition mechanisms can be used to migrate from IPv4 to IPv6 which includes dual stack networks, tunnels and translation technologies. Within all of this, network security is an essential element and therefore requires special attention. This paper analyses two transition technologies which are dual stack and tunnel. Both technologies are implemented using Cisco Packet Tracer and GNS3. This work will also analyse the security issues of IPv6 to outline the most common vulnerabilities and security issues during the transition. Finally, we will design and implement the dual stack, automatic and manual tunnelling transition mechanisms using Riverbed Modeler simulation tool to analyse the performance and compare with the native IPv4 and IPv6 networks.

KEYWORDS

IPv6, transition schemes, dual stack, tunnelling, security attacks, performance analysis, simulation, efficiency

1. INTRODUCTION

The IPv4 address space is quickly being exhausted, and there is a great need for a new protocol to overcome the lack of address space. It is for this reason that the new IPv6 protocol has been introduced, giving a larger address pool as it uses 128-bit address sizes. This means that there are many more addresses available than there are Internet-connected devices which mean that IPv6 is future-proof and allows for significant growth in internet technology. A further advantage is that there is no requirement for Network Address Translator (NAT) because each device is assigned a unique IP address. IPv6 has been designed with new features such as auto-configuration of addresses, improved the security, better quality of service (QoS) and a new header format [1]. It is due to this scarcity of address space that organisations are beginning the migration to IPv6 within their networks.

IPv6 and IPv4 are incompatible protocols, which means that interconnection between protocols is not available to network users, prohibiting them from connecting across networks. Therefore there is a requirement to use a transition mechanism(s) to allow for smooth migration and to allow IPv6 hosts to pass through IPv4 networks or connect with IPv4 hosts. The designers of IPv6 in the original specification (RFC 1752) defined the following transition criteria:

- It is simple to upgrade IPv4 hosts to IPv6 without disruption and can these be done without an upgrade of other routers or hosts which may be on the network?
- There are no dependencies which exist on other hosts or routing infrastructure when adding new IPv6 hosts.
- Both IPv4 and IPv6 addresses can be used in tandem without the need to upgrade all nodes at the same time.
- Upgrading IPv4 infrastructure to IPv6 requires little preparation, much like with deploying new IPv6 nodes.

There are a number of transition technologies which have been proposed and are widely use today such as dual stack and tunnel mechanisms. Due to the Internet services which widely use IPv4, it is important to know that

the transition from the previous protocol to IPv6 may take years to complete, and that means both protocols will be working together [2].

It can be said that changes in networks such as an upgrade to IPv6 may cause issues and may come at a high risk to an organisation. Network security is a very important aspect that should be looked at before migrating to IPv6. Moreover, most network security tools are designed and implemented to secure the IPv4 only. The scarcity of IPv6 related tools for network security analysis, as well as the lack of trained professionals, will lead to slow response times against network attacks.

The aim of this paper is to investigate the dual stack and tunnelling technologies while also looking at security risks of IPv6 and transition technologies. This will be accomplished by looking at both dual stack and tunnelling mechanisms in section 3, the translation security issues in section 4, the implementation and analysis of dual stack and tunnelling mechanisms along with IPv6 attacks in section 5, the performance analysis of various network scenarios in section 6 and final thoughts and conclusion in section 7.

2. BACKGROUND

This section examines the research which has already been conducted in IPv6 and looks at where further research is required. Despite the immature nature of IPv6, it has become a widely researched topic; however, one may say that there are still gaps in knowledge which have been generated by this research. In trying to accomplish the objectives of the research, the first element requires the IPv6 transition mechanisms to be defined, [3] an explanation for the scarcity of address spaces in IPv4 and extensive growth of the Internet in the past couple of years. Many kinds of systems and servers over the Internet have been developed based on IPv6 such as online shopping, Internet banking and trading stocks [4][5].

One can clearly identify the need for IPv6 addresses; however, the question remains as to what is going to happen to the existing IPv4 addressing schema? IPv4 and IPv6 are not able to work together in ways which would make them stable in a network environment and where they are able to interact easily with each other. The result is going to be the new IPv6 protocol being implemented alone, or both protocols will work together. Authors in [2] states that it is indispensable to maintain the IPv4 availability, to provide the inter-communication ability of IPv4 and IPv6. Most of the existing network applications are written for IPv4, but it is not very difficult to convert most IPv4 applications into applications compatible with IPv4 and IPv6 [6]. After realising the need of transition, the next section is to look for transition mechanisms. IPv4 to IPv6 migration can be divided two ways; aggressive and passive migration [7]. In the aggressive migration, IPv4 is directly disposed of and the whole infrastructure is replaced with IPv6. In passive migration, IPv6 is not ready so transition needs to be used and infrastructure of IPv4 is not discarded. Internet Engineering Task Force (IETF) has proposed many transition mechanisms to enable the networks to migrate to IPv6. There are several proposed mechanisms, with the best being tunnelling, dual stack and translation [1] [3] [5] [8] [9]. Dual stack mechanisms enable only similar network nodes to communicate with each other. Dual stack is the most extensively employed mechanism today.

In tunnelling mechanisms, IPv6 data is encapsulated within IPv4 packets and routed through IPv4 network(s). The source and the end points of the tunnel have to be dual stack [10]. Authors in [3] explains about the design and implementation of smooth transition mechanism based on tunnelling and translation technology and what characteristic features transition mechanism should possess. Peng Wu and Chris Metz explain about the tunnelling based route optimisations stating what should be done in optimising the tunnel transition mechanisms.

Once transition mechanisms have been examined, the following section will research the security aspects with regards to the transition mechanisms which are in place to avoid the threat of attacks to secure the end-to-end connection. During the IPv4 to IPv6 transition, both IPv4 networks and IPv6 networks will coexist. In this situation, the security risk and attacks are expected to increase. Caicedo and Joshi studied the security issues of IPv6 and outline the challenges in deploying and migrating to IPv6. They have divided IPv6 attack to four types which are reconnaissance, host initialization and associated, multicast-based, and attacks using routing header attacks [11]. IPv6 provides an integrated security through IPSec protocol which is mandatory for IPv6 networks. IPSec defines two types of security through authentication header and encapsulated security payload [12]. IPSec in tunnel makes source address validation for the IPv4 packet but does not verify the contents of

the payload where the IPv6 address is carried. Authors in [13] proposed a new mechanism to avoid and remove the spoofing attack in IPv6 over IPv4 tunnel using IPSec in transport mode. Many firewalls need to be coordinated and consistent to be properly managed, because the firewalls have separate rule sets for IPv4 and IPv6 which avoid inadvertent security exposure and intentional attack. The paper [14] outlines the effectiveness of conventional network security tools used to detect anomalies occurring on transition mechanisms. It further goes on to prove, using simulations, what can be the threat in IPv6 transition using the standard firewall and protection against the network attack. They found that automatic tunnel mechanisms are less secure than configured tunnels. However, Ting Liu and Yu Qu discussed a serious vulnerability in terms of worm propagation in IPv6 and dual-stack networks.

Before the transition mechanism(s) can be applied to large-scale deployment, systematic and quantitative performance analysis should be carried out [2]. Based on IPv6 transition technologies, Wu and Zhou [8] used three kinds of transition mechanism to analyse and test the performance; the three mechanisms are dual-stack, ISATAP tunnel and 6to4 tunnel. The result shows that within a dual stack environment, IPv6 has better performance than IPv4, ISATAP and 6to4 mechanisms [8]. Also, Shaneel and Sotharith [10] have evaluated the performance of configured tunnel and 6to4 tunnel. Both mechanisms are implemented on two Windows Servers; they measured performance metrics such as delay, throughput, CPU usage and jitter. The results obtained on the test-bed show that jitter values and TCP/UDP throughput of the two mechanisms are similar, but delay and CPU reading are significantly different depending on the choice of transition mechanism and operating system [10]. Moreover, Junaid and Javed [15] made an empirical evaluation of three commonly used transition technologies which are dual stack, manual IPv6 in IPv4 tunnel and automatic 6to4 tunnel. Finally, they made comparison of performance metrics with the native IPv6 environment. The results have shown that IPv6 network suffers a minimum delay and produces a higher throughput.

3. TRANSITION TECHNOLOGY

To provide an eventual transition to IPv6 only infrastructure and to currently coexist with IPv4 infrastructure, various transition mechanisms are proposed by IETF. Tunnel and dual stack are the most common technologies used while IPv6 translation [14],[16].

3.1. IPv4/IPv6 Dual-Stack

Dual-stack technology means IPv4 and IPv6 protocol stacks exist simultaneously on terminal devices and network nodes. Dual-stack architecture can receive, process, and forward data for both IPv4 and IPv6 nodes separately without making any change to the packet header. Also, it is one of the simplest transition technologies used today [5]. Figure 1 shows the operation of dual-stack technology.

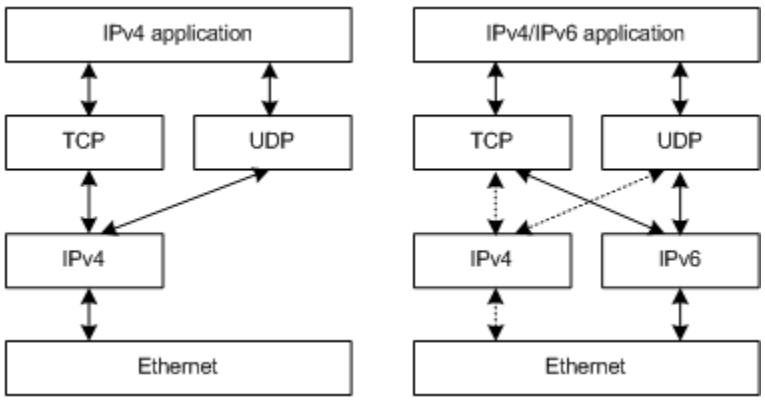

Figure 1. (a) Single Stack (b) A Dual Stack Architecture [15]

The interface of the device configured as dual-stack can have IPv6-only or IPv4-only or both addresses. The router contains two routing tables, one for IPv4 addresses and one for IPv6 addresses. When a dual-stack node receives a data segment, the node checks the packet header at the link layer. If the packet header is IPv4, the packet is handled by the IPv4 protocol stack. If the packet header is IPv6, the packet is handled by the IPv6

protocol stack. As to end hosts, modern computer operating systems have implemented dual-stack protocol [2].

3.2. Tunnelling Technology

Tunnels provide a method to carry IPv6 traffic to other IPv6 networks over an IPv4 network infrastructure. There are two types of tunnel which are configured and automatic tunnels, however, the IPv6 packets are encapsulated within IPv4 packets as shown in figure 2, and then IPv6 data can be transmitted through IPv4 networks [2]. The source and the destination points of the tunnel have to be IPv4/IPv6 dual stacked nodes [5].

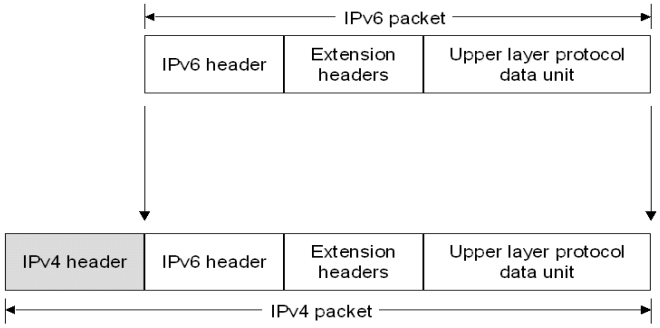

Figure 2. Format of IPv6 packet in Tunnel

The following tunnelling configurations are defined by RFC 2893 – this allows for the tunnelling of IPv6 traffic between the nodes across an IPv4 only infrastructure [17]:

- **Router-to-Router**

Within the dual stack environment, the router-to-router tunnel will be created which connects IPv6 nodes by way of IPv4 infrastructure. With the use of the logical link between the source and destination routers, communications are possible as in figure 3.

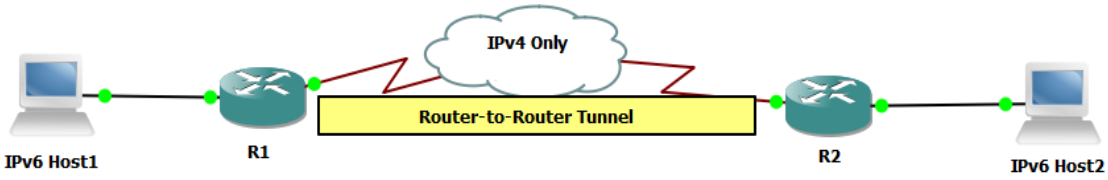

Figure 3. Router-to-Router Tunnel

- **Host-to-Router or Router-to-Host**

The IPv6 node which is placed within an IPv4 infrastructure will create the IPv6 over IPv4 tunnel to reach the IPv6/IPv4 router. The tunnel begins at the host and finishes at the router or vice versa as in figure 4.

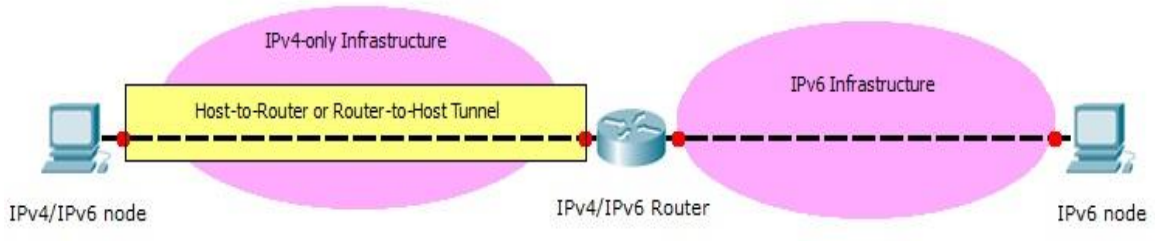

Figure 4. Host-to-Router or Router-to-Host tunnel

- **Host-to-Host**

The IPv6/IPv4 node which is residing within the IPv4 infrastructure will create the IPv6 over IPv4 tunnel. The tunnel spans from the source to the destination nodes as in figure 5.

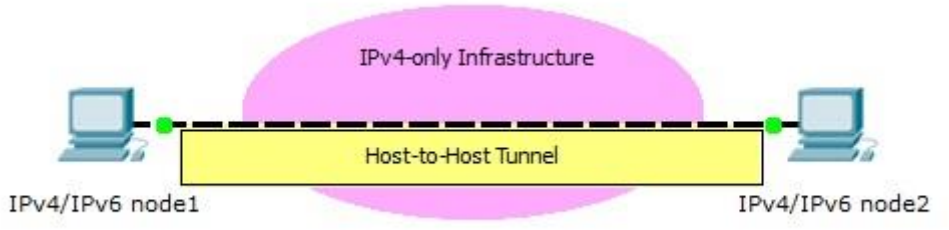

Figure 5. Host-to-Host Tunnel

3.2.1. Configured Tunnels

Within the tunnelling environments, the IPv6 packets which are sent from the originating node are encapsulated within an IPv4 tunnel. At the end point, the packets are decapsulated into IPv6 traffic. The configuration information which is stored at the endpoint of the tunnel will determine the addresses. Configured tunnels can be placed within a router-to-router, host-to-router/router-to-host or host-to-host environments.

3.2.2. Automatic Tunnels

The difference between automatic and manual tunnels lies in that there is no need to pre-configure tunnels and nodes; all nodes automatically set up the tunnelling procedure [18]. There are many types of automatic tunnels:

3.2.2.1. 6to4

The 6to4 method allows for connection to exist between two IPv6 domains where an IPv4 network resides between them. The IPv4 addresses are part of the IPv6 addressing schema while the packets are being transferred as IPv4 is the link. The 6to4 procedure has a unique prefix: 2002: IPv4 address::/48. This procedure works within the router-to-router configuration.

3.2.2.2. 6over4

Where a network consists of IPv6 capable hosts and routers but the network operates within IPv4, 6over4 will treat the IPv4 network as a virtual Ethernet for IPv6 communications. IPv4 multicast is used to tunnel the IPv6 packets.

3.2.2.3. ISATAP

ISATAP (Intra-Side Automatic Tunnel Addressing Protocol) uses an address assignment for automatic tunnelling which is used within the unicast IPv6 connectivity. This is most used where IPv6 and IPv4 hosts exist within an IPv4 intranet. ISATAP is not able to support multicasts as it uses Non-Broadcast Multi-Access (NBMA) communication model. ISATAP addresses use the locally administered interface identifier ::5EFE:private unicast IPv4 address, or ::200:5EFE:public unicast IPv4 address.

3.2.2.4. Tunnel Broker

The tunnel broker acts as a tunnel creation mechanism between two nodes within network environments. This is a simple form of automatic tunnelling which only requires there to be a web server and client-side authentication to gather details such as IP address, operating system and IPv6 compatibility. Figure 6 shows the tunnel broker mechanism.

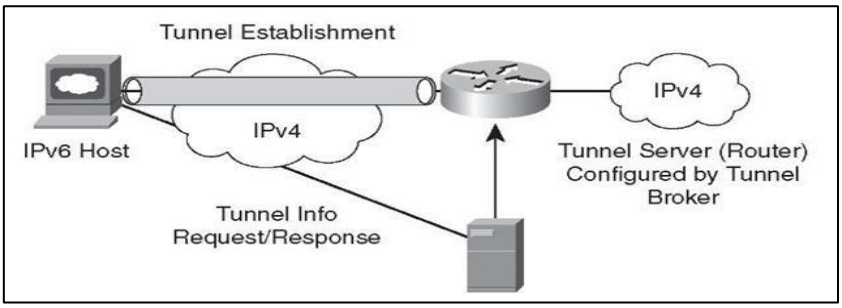

Figure 6. Tunnel Broker mechanism [24]

3.2.2.5. Teredo

Teredo assists in providing an IPv6 over UDP connection where the IPv6 host is behind a NAT router without a unique public IPv4 address. Teredo is a mechanism which aids interfacing IPv6 nodes by use of the internet. IPv6 nodes may be connected to IPv4 internet through NAT devices.

4. SECURITY ISSUES

Before any migration or dual stack environment can be installed with IPv6, all the security aspects and implications which exist must be looked into to avoid network disruption. Due to the new nature of the IPv6 technology, these risks are higher than ever [14]. The securities issues need to be looked into consist of IPv6 protocol issues, transition mechanisms and the IPv6 deployment issues.

4.1. IPv6 Protocols Issues

Because there are many differences in features between IPv4 and IPv6, there are many new security issues which must be looked into. Some of the features which cause significant security issues have been further discussed below.

4.1.1. Extension Headers

Extension headers, simply, are a header placed on packets which are sent through the IPv6 network. These headers can be chained together to allow one header to point to another. Needless to say, all IPv6 nodes must be capable of accepting packets and reading the relevant headers. Currently, there are six extension headers which have been defined. It has been defined that "IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet" [19].

There are some security flaws with extension headers which may allow users to avoid access based control systems and also due to the nature of the headers it is also possible for an intruder to send a packet to a public address containing a forbidden address. Spoofing packets in these ways may lead to a denial-of-service (DOS) attack and therefore causes issues for all nodes on the network (Martin and Dunn).

The first method by which extension headers can be used maliciously is where an attacker uses a long chain of headers such that security devices are no longer be able to get to the transport layer for the deep packet inspection to be carried out [20].

The issue with this technique and many like it is that they are compatible with the IPv6 specification and therefore routers are not able to stop them. It is of the utmost importance that security policies are implemented to mitigate these risks.

Within IPv4, deep packet inspection ensures that all packets which contain damaging and unknown options, therefore extending this service to IPv6 will ensure the same security. However, this is inconsistent with RFC2406 (IPv6 Specification) which makes it a requirement for hop-by-hop options only. The specification also does not allow for headers to be processed in any other way than has been shown in the packet itself. The specification, therefore, does not take account of middleboxes and their behaviour which puts a limit on packet inspection policies.

4.1.1.1. Hop-by-Hop Extension Headers

Another important element which must be examined with regards to extension headers is the hop-by-hop extension header which is used to carry information which must be looked at by every node within the delivery path of the packet. The option header is defined by the Next Header value of 0 in the IPv6 header.

The benefit of hop-by-hop option headers is that they can have any number of hop-by-hop options with certain options appearing multiple times within the chain. Attackers can use inconsistent option values or invalid options which can lead to 'Parameter Problem' ICMPv6 error messages. In certain circumstances, the attacker may be able to burden the router to the point that a DOS attack is created [19][20]

4.1.2. Fragmentation

IPv6 by default does not prohibit the reassembly of overlapping fragments even though this is a well-known security threat which can be used to avoid firewalls. In IPv4, mitigation measures were in place allowing the dropping of fragments with an offset of one byte. However, this option is not available with IPv6 due to the header containing any number of extension headers.

Due to this, overlapping fragments are now not allowed to be sent within an IPv6 environment because non-threatening nodes no longer have the need to send overlaps. However, fragmentation is still possible only from the source node which makes the path MTU discovery method an obligation. The minimum requirement which has been suggested for MTU size is 1280 octets and therefore anything below this should be dropped unless the packet is the last to come through [20].

Intruders into the network may not be able to find port numbers in the first fragment and thus can bypass security monitoring devices expecting to be within the transport layer. Alternatively, an intruder may be able to send a large number of smaller packets causing an overload on the resources and creating a DoS attack. These risks can be mitigated by implementing a limitation on the total number of fragments and allowing space between their arrival times [20].

4.1.3. Auto-configuration

Auto-configuration is a method of automatically generating the address for a node which is placed on an IPv6 network. With the introduction of more devices into a network, auto-configuration allows the network to run without the DHCP server. IPv6 nodes can configure themselves through either stateless or stateful configuration. The stateless auto configuration will generate an address based on the network prefix which is obtained from the router and the MAC address of the node. Stateful autoconfiguration, on the other hand, uses a DHCPv6 server to gain an address.

Stateless auto-configuration is one of the key features of IPv6. However, it does have a lot of network vulnerabilities and security concerns attached to it as in figure 7. One of the major concerns is the trust model which is the network and node trust within the environment. The issue with the SLAAC (Stateless Address Autoconfiguration) system is that any node can acquire an address without approval or control and this, therefore, opens the network to external threats. A node is also able to acquire the global prefix and router advertisement using ICMPv6 messages for Neighbour Discovery (ND). This can, therefore, build a globally routable address which can be set up without approval [11][14][19]. The following types of attacks are therefore made possible due to this security flaw:

A. **Malicious Router:** a device on the network may work as a man-in-the-middle and act as the router link advertising itself and allowing connections. It can then gather the information which is being passed over the network.
B. **Attack on a legitimate router:** a malicious device on the network can take the legitimate router out of action and act itself as a router. Alternatively, the malicious device can attack the router to change its configuration.
C. **Bad prefixes**: a malicious device can advertise itself as a router and then advertise bad prefixes which are not on the link. All hosts which use auto configuration will then have an invalid address.
D. **Failure of DAD and NUD Processes:** a malicious node is able to reply to DAD with an NA packet and prevent new nodes from joining. The NA packet sends information claiming that it is already using

the address which has been requested. In the same way, it is possible for the malicious device to falsely respond to NUD messages causing an NUD process failure.

E. **Non-existent address:** an external host may be able to send traffic to a legitimate looking address however it will carry an invalid interface ID. The machine will try to resolve the issue and therefore spend resources doing so, making it vulnerable to a DOS attack.

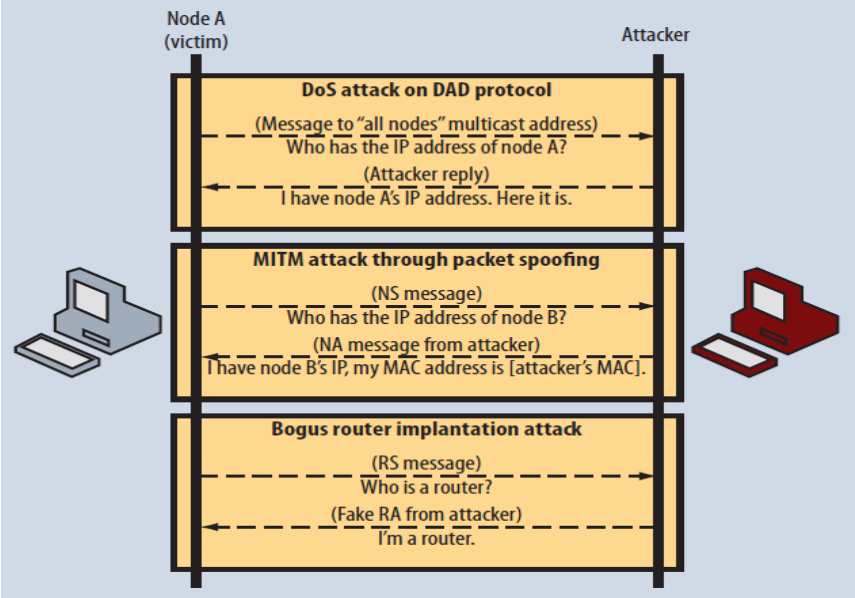

Figure 7. Attacks on IPv6 autoconfiguration process [11]

4.1.4. Multiple Addresses

IPv6 allows the assignment of multiple addresses to an interface, however, due to address based filtering no longer being an option due to the auto configuration, a firewall has to be able to learn the addresses dynamically and therefore all filtering rules need to be generated automatically using a high-level policy rule-set. Unfortunately, this is not an option which is available and therefore leaves networks vulnerable. Identification tokens are another option to identify hosts. However, ISO layer 3 does not have this capability [25].

4.1.5. Multicast-Based Networks

IPv6 a multicast network eliminates broadcasting of addresses and instead employs the multicast heavily. An attack on a multicast network can obstruct the ability of a node to operate. A DOS attack is very easily done by sending messages to the group addresses informing all members that they must leave. IPv6 also adopts standard multicast addresses for important devices such as routers and DHCP servers; any attack which is placed on these devices can be done by modifying messages directed to these addresses and thereby assists in receiving information from the systems.

4.2. Transition Technologies Issues

It is important to build an in-depth understanding of security issues of transition mechanisms as this may assist network administrators in applying the appropriate security mechanisms within the network. This section is concerned with dual stack and tunnelling mechanisms.

4.2.1. Dual-Stack

When a dual-stack environment is set up, it must be ensured that the devices which are on the network have adequate security to mitigate the risk of attacks in both IPv4 and IPv6 environments. Hosts will therefore control firewalls, VPN clients and IDS/IPS systems and these must be able to inspect traffic from IPv4 and IPv6 and block any unauthorised traffic independently of each other. The network administrators within an environment should consider implementing IPv6 only firewalls which can secure the network the same way it would be secured in the IPv4 network [14].

4.2.1.1. Dual Stack Worm

There has been a recent discovery of the IPv4-IPv6 dual-stack-worm which can detect victims who are within the same IPv6 subnet using multicast scanning. At the same time it can scan targets within a different IPv6 subnet or scan within IPv4 only networks using random scanning. The worm will find any hosts on the network which are vulnerable and infect them by exploiting vulnerabilities in the systems. Figure 8 shows the attack strategy and propagation strategy within a dual stack environment of the IPv4-IPv6 dual-stack-worm [22].

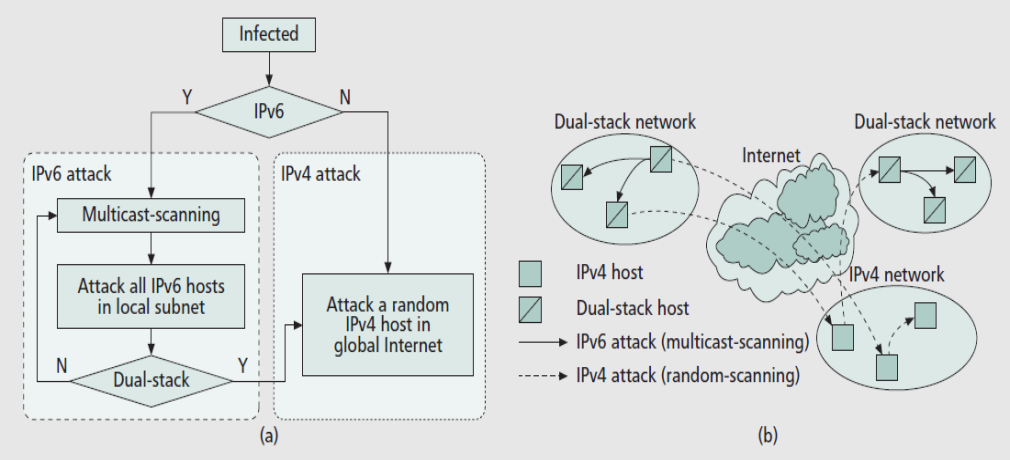

Figure 8. IPv4-IPv6 dual-stack worm: (a) Attack strategy (b) Propagation in the hybrid network [22]

4.2.1.2. Quality of Data Transmission

An important aspect which must be considered when looking at IPv6 deployment with respect to both tunnel and dual stack transition mechanisms is the quality of data transmission. The most common method in which this can be checked is to use the ping and traceroute towards IPv4 and IPv6 dual-stack sites to know the round trip time (RTT). A common issue which is seen here is that when tunnels are set up for experimentation or when tunnels have been badly configured, it leads to a loss of quality within the data transmission seen by a longer RTT. This is due to the number of tunnel connections which are implemented in certain scenarios.

4.2.1.3. Handling Multiple Responses

The issue of how configurations information should be handled is another concern. These may be gathered from multiple sources and can exist where there are both DHCP and DHCPv6 servers, that is, two physical nodes or two servers running on the same node. A method by which the lists can be merged to show a list of addresses may also be required. Of course, nodes may opt to only use one of the servers and only where no answer is received will they follow up with another.

Merging can certainly be accomplished. However, it may pose some complexity. There may reside issues of priority or the storing and usage of the nodes.

4.2.1.4. Different Administrative Management

There are cases in which IPv6 services may be administered and managed by different organisations or people. This is most likely going to be the case where a wireless environment exists. This does, however, pose a problem for consistency of data which is offered by each DHCP version. The protocols by which each client connects may be different, and therefore clients may gain an advantage from this administrative domain.

4.2.1.5. DNS Load Balancing

Administrators may often choose to opt for DNS server information lists for load balancing. However, each node will give different responses to different clients. Responses which are from different DHCP versions may make matters of configuration complex if the knowledge of the load balancing policies is not available to both servers.

4.2.2. Tunnelling

Due to the many tunnels which can be employed within a network environment, there are many security issues which present themselves. Namely, with automatic tunnel procedures because there is no destination set in place therefore more vulnerabilities which may present themselves. [23] Both configured and automatic tunnels with their issues are discussed below.

4.2.2.1. Configured Tunnels

Firstly, it must be said that configured tunnels are more secure than automatic tunnels because each tunnel which is configured will be set up with both source and destination. The issue however lies in the open port between the IPv4 and IPv6 networks; the concern lies in the firewalls and the data which is passed between them. Currently, there is no way of authenticating any users or information which is passed through the two networks, therefore leaving either or both network(s) in a vulnerable position. The only way in which it is possible to authenticate is to look at the source IP address. However, packets are then subject to exploits such as IP spoofing and injection packets at the endpoints of the tunnel.

4.2.2.2. Automatic Tunnels

As has been previously mentioned, automatic tunnels are not as secure as manually configured tunnels. Automatic tunnels are easily affected by packet forgery and DOS attacks because there is no preconfigured endpoint. The network architecture must therefore provide mechanisms which can protect against IPv4 and IPv6 vulnerabilities. The security of tunnelling mechanisms is discussed below [18]:

4.2.2.2.1. 6to4

As defined in (RFC 3964), 6to4 is susceptible to the following attacks: ND messages, spoofing; reflecting, IPv4 broadcast attack.

4.2.2.2.1.1. Attacks with ND Messages

The 6to4 router works in a way that it will assume that all the routers and relays are “on-link” and therefore it is possible to attach with ND messages from the IPv4 network (this is on the assumption that there has been no prior trust relationship established). The attack will target the 6to4 pseudo-interface, using link-local addresses, and as long as the 6to4 addresses have not been used in the source or destination there are no security checks on these packets.

4.2.2.2.1.2. Spoofing Traffic

Both IPv4 and IPv6 nodes can be a victim of this attack, which would involve the packets being modified in some way by the node and then sent to the target addresses. This attack can then lead to a DOS attack. Although DOS attacks in this way is not a new thing, what makes DOS attacks in this scenario obscure is that the source of the spoofing is much more difficult to locate as the 6to4 router does not log the IPv4 addresses, therefore hiding the address of the attacker.

4.2.2.2.1.3. Reflecting Traffic to 6to4 Nodes

Reflecting traffic is very similar to spoofing traffic; however, in this case the spoofed packet is sent to an IPv6 node either originating at an IPv4 node through a 6to4 relay or an IPv6 native node.

4.2.2.2.1.4. Local IPv4 Broadcast Attack

This attack only applies to 6to4 routers where they do not check whether the IPv4 address of the router which is receiving the encapsulated IPv6 packet is a local broadcast address or a multicast address. This attack occurs where a 6to4 node attempts to send a packet to an address which corresponds to the broadcast address remotely. Another attack which can be initiated is where an IPv4 node not belonging to the local network sends traffic with an invalid source address. The 6to4 router would then respond by sending ICMPv6 packets to the source, thereby creating a DOS attack.

4.2.2.2.2. ISATAP

Much like 6to4, ISATAP employs headers to send information from one protocol version to another and therefore it is susceptible the same types of risks which have been discussed in 6to4.

4.2.2.2.3. Teredo

Teredo relies on the endpoints of the tunnel to encapsulate and decapsulate packets, therefore any host which is within the LAN, which refers to *any* host behind the firewall, is able to encapsulate and decapsulate packets. It is difficult to secure all endpoints and therefore a single firewall would be required to secure the network. However, because the packets are encapsulated, it is impossible for the firewall to read the information within the packets. Therefore packet spoofing is still a concern.

4.2.2.2.4. Tunnel Broker

Much like the previous mechanisms, packet spoofing is a serious concern; however, in this scenario the firewalls and other security systems are sometimes placed quite far from the source and destination endpoints, therefore, response times are increased while availability and confidentiality are significantly decreased. A malicious user can easily exploit the network by requesting multiple tunnels and depleting the resources of the network, thereby creating a DOS attack.

4.3. IPv6 Deployment Issues

Most new devices are coming with IPv6 compatibility and do not come in an IPv6 only form. It is important that all IPv6 technologies are thoroughly tested and it is ensured that all data which is passing over is secure and free from spoofing or other such attacks which could cause harm to either the network or its users. The administrators must ensure that all transition mechanisms are considered when looking at security policies.

There are issues such as DNS servers, addressing schemes and multiple address registrations which require proper observation with the current technologies; therefore time must be invested into working out a solution such that time can be saved with managing the network. Certain operating systems by default have IPv6 functionality enabled. However, the technology behind the hardware is not capable of IPv6 traffic, therefore causing security issues.

Due to all these issues, it is important that not only network administrators but also staff are trained on the procedures and security matters with regards to IPv6. A method in which one can ensure the security of a network is to use the software which has been proposed in the research by Lai [27]. This software can assist in looking through the IPv6 network and determining whether the security devices which have been implemented are secure. The software will launch a virtual machine, followed by a series of attacks which can be done using different tools. Finally, the software will generate a report and it will show the network administrators whether the network is secure or not; if it is proven to be insecure, it will provide suggestions as to how network administrators may solve the vulnerabilities.

5. IMPLEMENTATION OF TRANSITION SCHEMES AND ATTACKS

This section looks at the transition technologies implementation and looks at the possible attacks which can be done on IPv6.

5.1. Dual-Stack implementation

In this paper, dual stack network are designed and implemented using Cisco Packet Tracer software. This section intends to analyse the implementation strategy of the dual stack network, paying attention to Cisco Router implementation and the two methods of dual-stack that can be used.

5.1.1. Router Dual Stack

Within the network, two routers are connected through serial ports with two nodes on each router, one which is in IPv6 and the other in IPv4 address; this is the setup of a router dual stack network where the router can

forward data from both protocols. The network addresses and routing paths will be determined once it is clear which protocol the hosts are using. The IP forwarding function will then be configured on each router to allow for information to travel over the networks. Figure 2 below shows the results of the Cisco Packet Tracer:

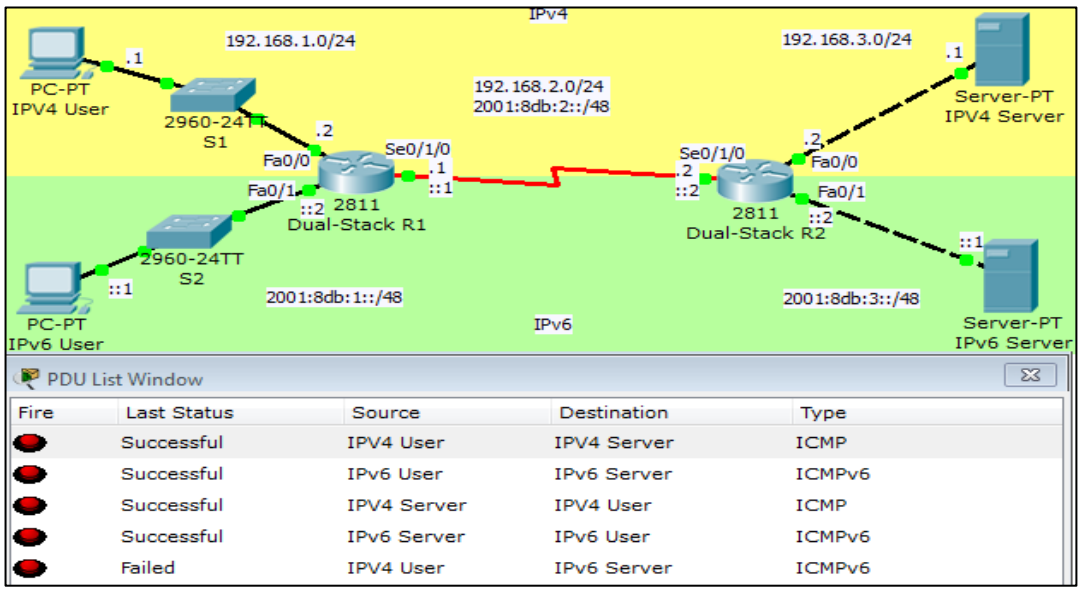

Figure 9. Router dual-stack network

Figure 9 shows that both IPv6 nodes can communicate with each other and both IPv4 nodes also can communicate with each other. However, IPv6 node is unable to communicate with another IPv4 node.

When a new host is connected to the switch S1, the host must be IPv4, despite the router being dual stack, because Fa0/0 is configured with an IPv4 address only. Likewise, if a new host is connected to S2, the host must be IPv6 because Fa0/1 is configured with an IPv6 address only.

5.1.2. Router and Application Dual Stack

Similar to the previous scenario, an IPv4 and an IPv6 user exists, however, as opposed to IPv4 and IPv6 servers being implemented, only one dual stack server exists.

As mentioned previously, where the fast Ethernet port is only configured with one address for one protocol, only hosts using that protocol can connect. Where in this scenario the fast Ethernet port is configured with both IPv4 and IPv6 addresses and connected to a switch, any new host which joins the network is able to communicate with the server regardless of the protocol they are using. This has been shown in figure 10.

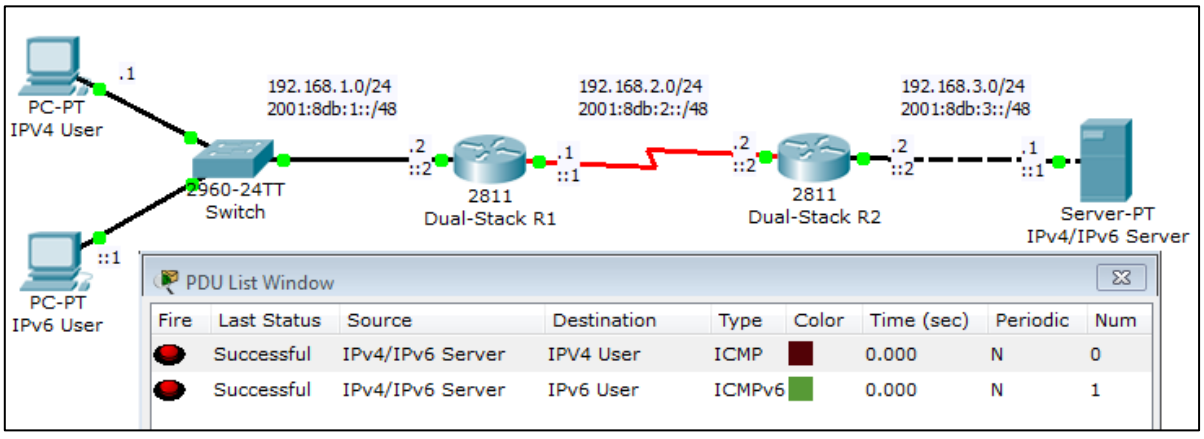

Figure 10. Routers and server dual Stack

5.1.3. Results

From the experiment conducted as per the above, it can be concluded that, with regards to the router dual stack, only hosts which are working on the same protocol can communicate with each other. In the router and application dual stack, however, with the server running dual-stack as well as the routers, both IPv4 and IPv6 hosts are able to communicate and access the server.

5.2. Tunnel Implementation Method and Analysis

As has been explained above, tunnels have many vulnerabilities which need to be investigated, in particular, the 6to4 tunnel which has vulnerabilities to sniffing, spoofing and DOS attacks.

5.2.1. Method

In the experiment, two dual-stack routers with one IPv4 router between them is used. The dual-stack routers are connected to two hosts on each network independently. This has been shown in figure 11.

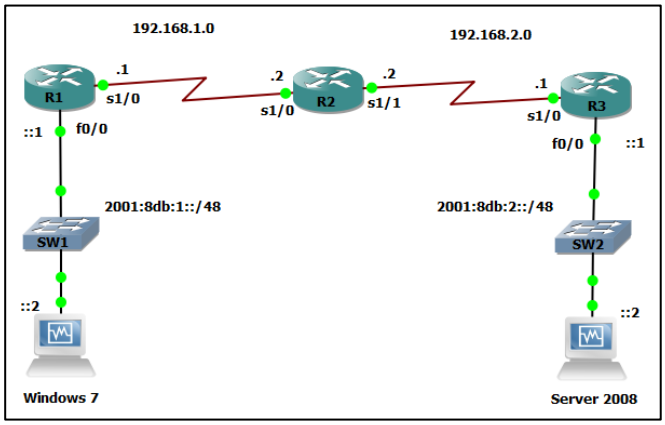

Figure 11. Network topology

A 6to4 tunnel is created between R1 and R3 for the two IPv6 networks to communicate through the existing IPv4 network. In doing this, the serial ports on all routers are assigned an IPv4 address, while the two IPv6 networks are connected via fast Ethernet ports on routers R1 and R3 which are assigned IPv6 addresses.

Data will be sent from the Windows 7 host to the Server 2008 host through the 6to4 tunnel and packets will be captured anywhere between the start and end points of the tunnel.

5.2.2. Results

Given the method used above, the Wireshark packet capturing software was used to analyse data which was sent between the IPv6 networks. The analysis of a packet within the tunnel shows that both IPv4 and IPv6 protocols exist within the same ICMP message which proves that the IPv6 packet is encapsulated within the IPv4 tunnel as an IPv4 packet. This is shown in figure 12.

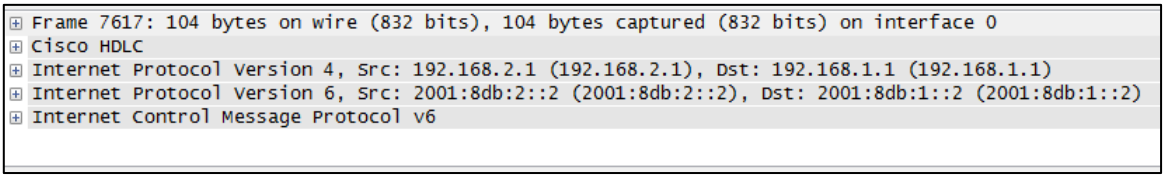

Figure 12. ICMPv6 Frame

Looking at this packet in detail in figure 13, the IPv4 segment of the header is analysed. The source and destination (as highlighted in figure below) have been clearly shown within the packet; however, the source and destination only refers to the start and end points of the tunnel and not the source and destination of the original IPv6 packet. The analysis also shows that protocol type 41 was used to send the IPv6 packet over the IPv4 network, a requirement of 6to4 tunnels.

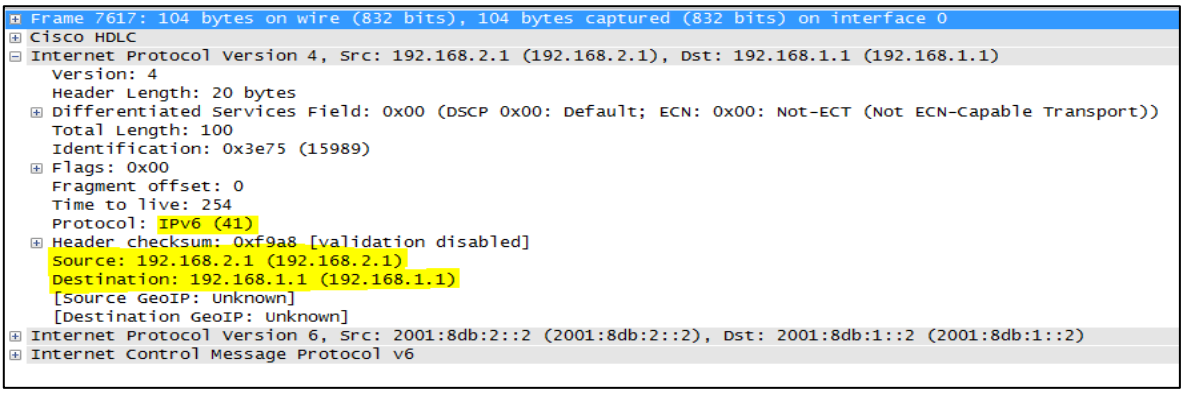

Figure 13. IPv4 header

Upon analysis of the IPv6 header in figure 14, it is clear to see that the source and destination of the IPv6 addresses are available. This is unlike the IPv4 header analysis where only the IPv6 source and destination are available.

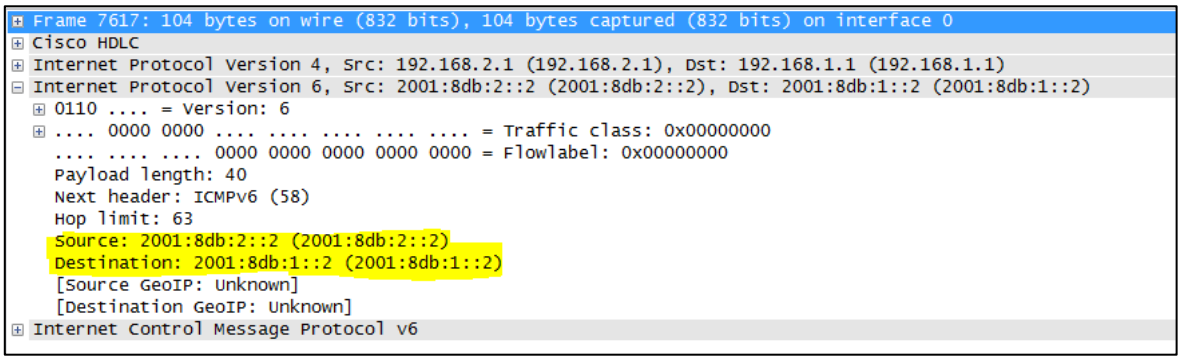

Figure 14. IPv6 header

The experiment has clearly shown that not only is a sniffing attack possible within the 6to4 environment but is also possible to gain access to source and destination information of packets. This leaves the network vulnerable to spoofing attacks which allow the malicious user to modify easily IPv6 source and destination addresses which are encapsulated in the tunnel.

5.3. Implementation of IPv6 Attacks

The previous sections have provided much information on the security vulnerabilities which exist within each technology and the possible attacks which can be carried out. This section looks at the attacks and demonstrates the tools which can be used to carry out new attacks like host probing, fake router, flooding and spoofing attacks.

5.3.1. Method

In order to carry out this experiment, three Virtual Machines were set up and connected using Debian, Windows Server 2008 and Windows 7 operating systems. This can be seen in the figures 15, 16 and 17.

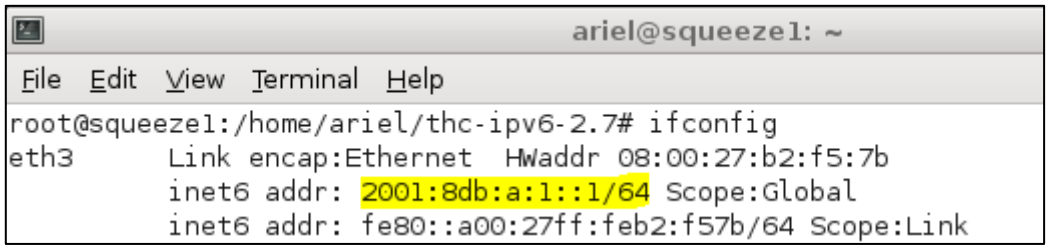

Figure 15. Debian IPv6 Address

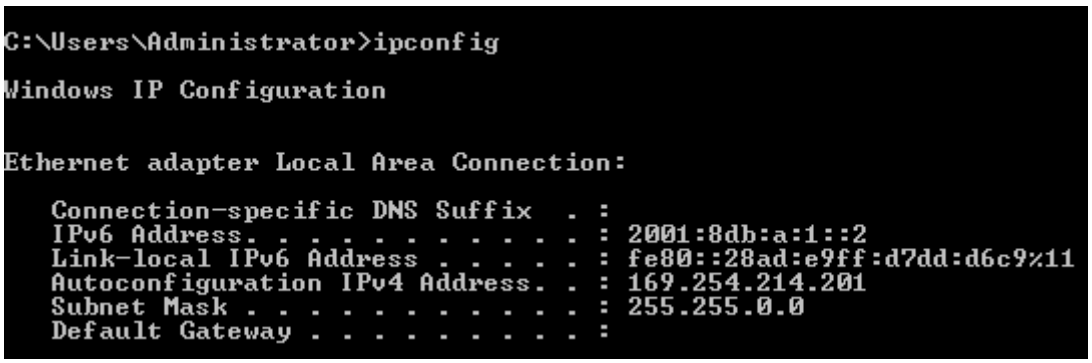

Figure 16. Windows 7 IPv6 Address

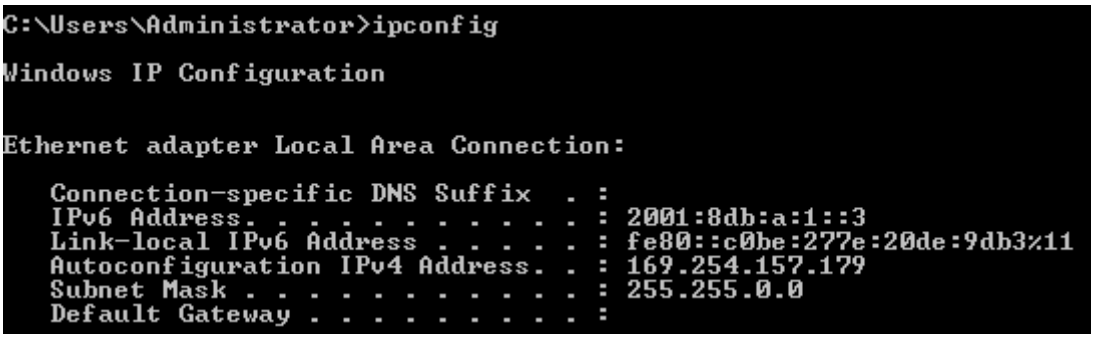

Figure 17. Windows Server IPv6 address

The Debian machine was used to simulate the attacker on the network. The following list of tools was installed on the machine:

Table 1. Attack tools [26]

Tool Name	Description
6to4test	This little script tests if the IPv4 target has a dynamic 6to4 tunnel active
inject_alive6	This tool answers to keep-alive requests on PPPoE and 6in4 tunnels; for PPPoE it also sends keep-alive requests.
alive6	Shows alive addresses in the segment. If you specify a remote router, the packets are sent with a routing header prefixed by fragmentation
covert_send6	Sends the content of FILE covertly to the target and its POC
detect-new-ip6	Detects new ipv6 addresses joining the local network.
detect_sniffer6	Tests if systems on the local LAN are sniffing.
dnsrevenum6	Performs a fast reverse DNS enumeration and can cope with slow servers.
dos-new-ip6	This tools prevents new ipv6 interfaces from coming up
dump_router6	Dumps all local routers and their information
fake_advertise6	Advertise ipv6 address on the network (with own mac if not specified), sending it to the all-nodes multicast address if no target address is set. Source IP address is the address advertised if not set.
fake_dhcps6	Fake DHCPv6 server. Use to configure an address and set a DNS server
fake_dns6d	Fake DNS server that serves the same ipv6 address to any lookup request You can use this together with parasite6 if clients have a fixed DNS server
fake_mld6	Advertise or delete yourself or anyone in a multicast group.
fake_mldrouter6	Announce, delete or solicited MLD router - yourself or others.
fake_router6	Announce yourself as a router and try to become the default router. If a non-existing link-local or mac address is supplied, this results in a DOS.
flood_advertise6	Flood the local network with neighbour advertisements.
flood_mld26	Flood the local network with MLDv2 reports.
flood_mld6	Flood the local network with MLD reports.

flood_router6	Flood the local network with router advertisements.
flood_router26	Flood the local network with router advertisements.
fragmentation6	Performs fragment firewall and implementation checks, including the denial-of-service.
implementation6	Performs some ipv6 implementation checks, can be used to test some firewall features too.
kill_router6	Announce that a target a router going down to delete it from the routing tables.
redir6	Implant a route into victim IP.
rsmurf6	Smurfs the local network of the victim.

The following tools were used to carry out this simulation: fake_router6, flood_router6, flood_router26, detect-new-ip6 and dos-new-ip6. We were not able to simulate attacks for all the tools due to the many attacks which exist. However, this shows the possibility of many attacks which can be carried out.

5.3.2. Results

The results of the simulation are discussed below.

5.3.2.1. New Host Probing

Using detect-new-ip6, the attacker's computer will listen for ICMPv6 messages on the network and respond to the attacker by showing the IP address of the newly connected device. In this scenario, the Windows Server and Windows 7 was disconnected and reconnected to the network. Upon reconnection, the tool detected a new device being connected to the network, as shown in figure 18. The hacker uses such software to start the first step of hacking which is to get the victim's IP address.

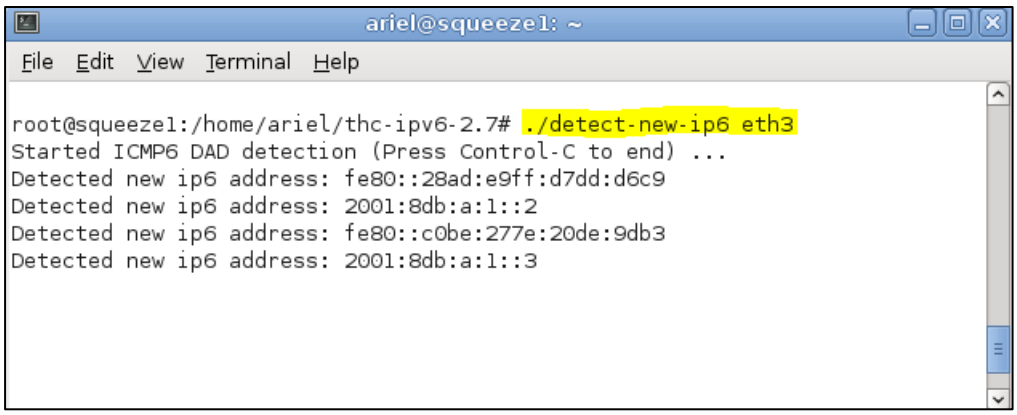

Figure 18. IP addresses for devices being connected

5.3.2.2. Malicious Router

Using the tool fake_router6, the attacker can send router advertisement packets to the network with the highest priority and make all devices on the network believe that it is the legitimate router, as shown in the figures below. This will allow the fake router to set the machine as the default gateway which allows the man-in-the-middle status. Please refer to Figures 19, 20 and 21.

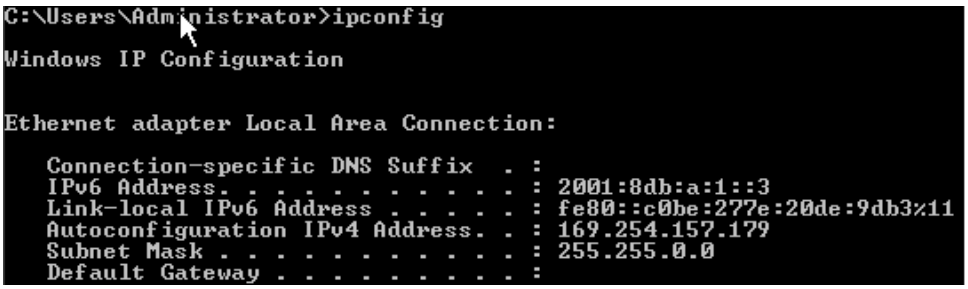

Figure 19. IPv6 address for Windows Server before running fake router

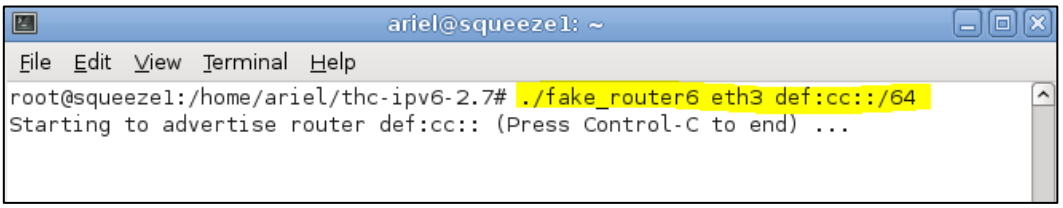

Figure 20. Starting fake_router6

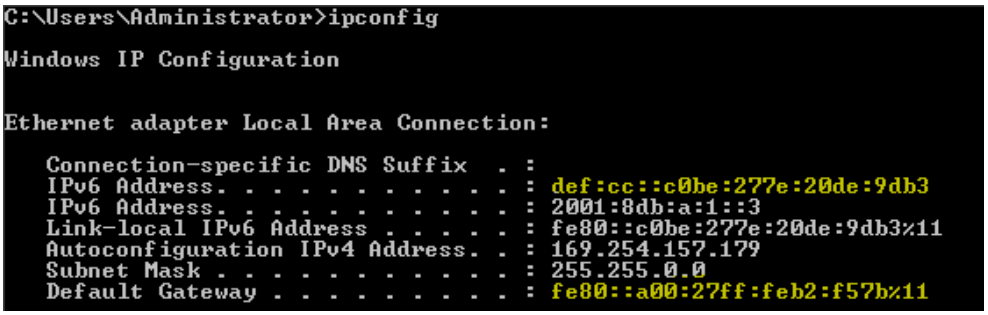

Figure 21. IPv6 address has been changed in both Windows machines

If the attacker gives a non-existent link-local address then it will be a DoS attack. Figure 22 and 23 show what the software can do.

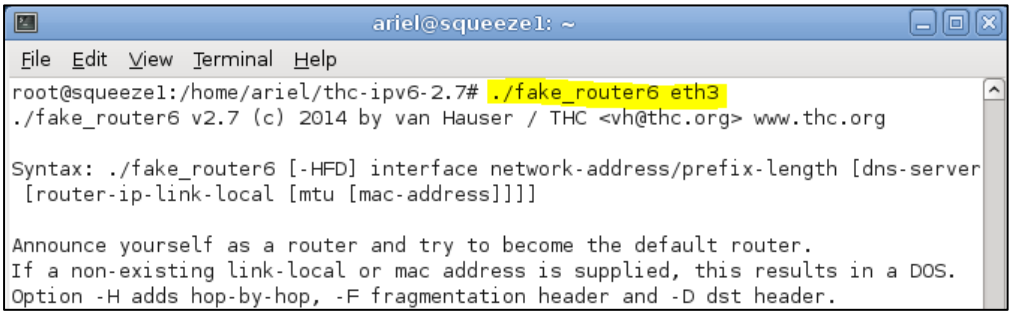

Figure 22. Run the tool with non-existent link-local address

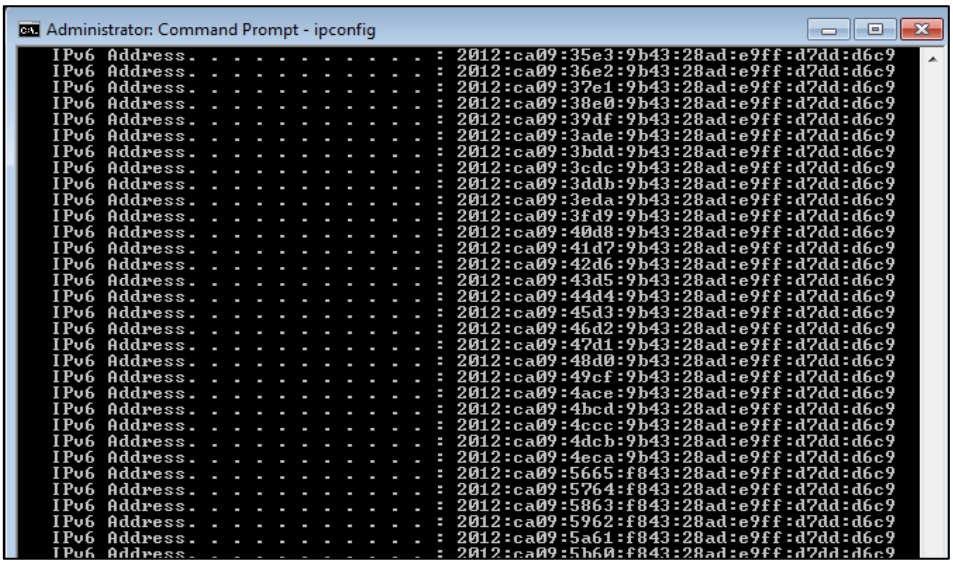

Figure 23. Result in victim machine

5.3.2.3. DoS Attack

Using flood_router6, the attacker is able to flood all devices on the network. As shown in figure 24 and figure 25, many thousands of packets are sent from the attacker's machine to the target hosts. Within 2 seconds all hosts which were connecting to the network are unresponsive as shown in figure 26.

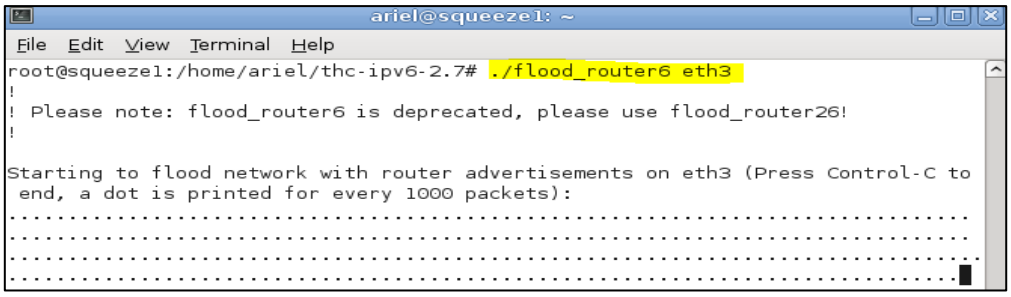

Figure 24. The old version of the flooding tool

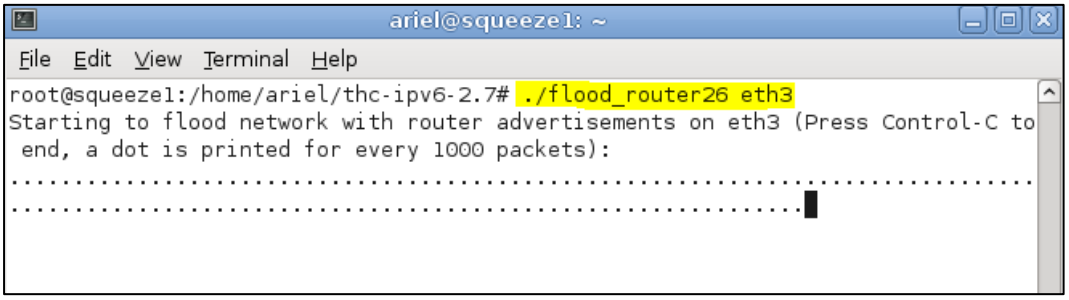

Figure 25. The new version of flooding tool

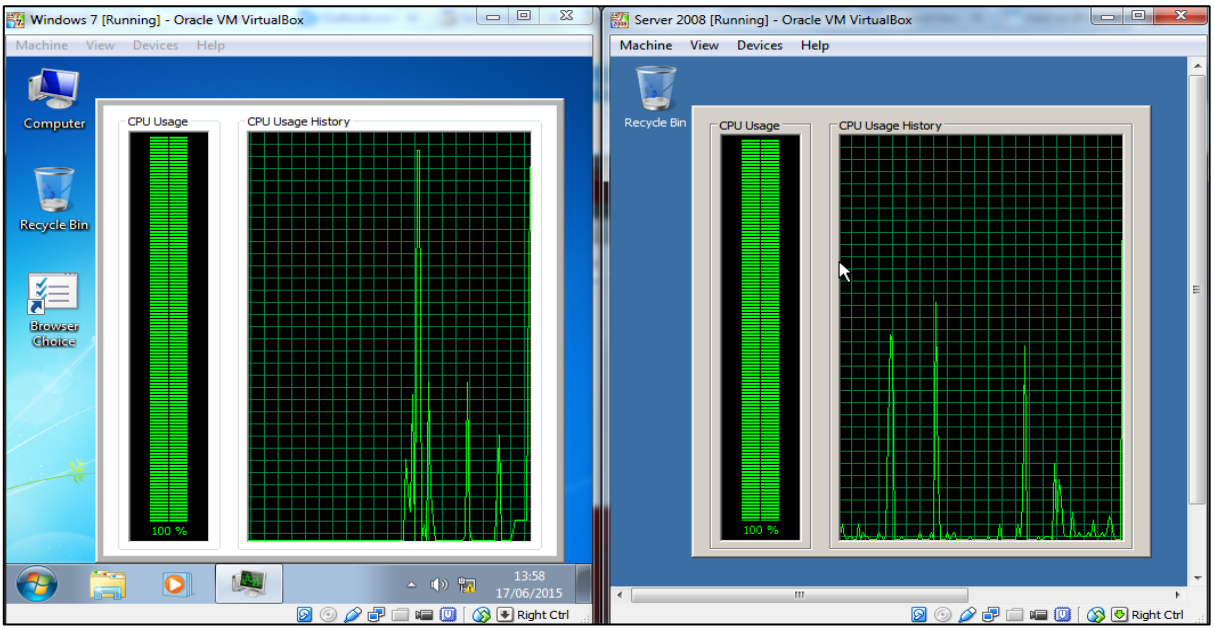

Figure 26. Result after running flooding tool

5.3.2.4. Spoofing Address

This tool is very similar to detect-new-ip6. However, this tool will listen for ICMPv6 DAD messages on the network and respond with a message to say that the IPv6 address already exists. In this way, no host will be able to connect to the network, thereby leading to a DOS attack. The attack tools and the result can be seen in the figures below.

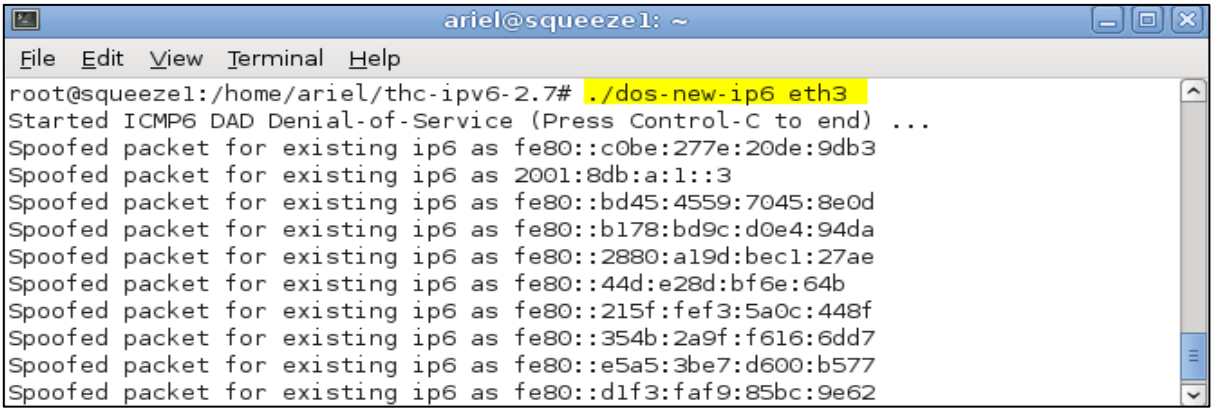

Figure 27. Command to run the software in Debian

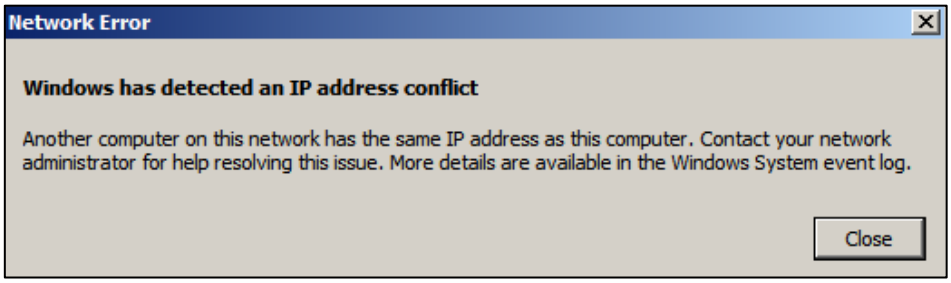

Figure 28. The target machines show a message (IP address is used)

5.3.3. Discussion

As can be seen from the information presented above, the tools and technique to attack any IPv6 network have already been developed. The attacks which were carried out were with ease and easy for anyone to replicate.

The only action required by the attacker is to run the program. So the attacks are very simple to carry out, and one would be able to carry out other attacks with the tools that have been shown in Table 1.

6. PERFORMANCE ANALYSIS

Within this section, the performance of the network which is shown below was carried out to understand the differences in the performance between native IPv4 and IPv6 networks with that of the dual-stack and 6to4 tunnel and manual tunnel; therefore four different scenarios were created using Riverbed. The reason this performance analysis has been carried out is to show the effects of each type of network on the hardware. This is an important factor which must be considered because stressing the servers too much can lead to a slow connection; network efficiency must be considered.

6.1. Method

As can be seen in the network topology in the figure 29, a total of six routers has been utilised, connected via serial ports. Router R1 and R6 are connected to a pair of switches by fast Ethernet ports. On the R1 side, each switch then connects to a LAN which consists of a number of hosts independently. On S3 and S4, an email and database servers are found respectively. The same network topology has been used in all scenarios.

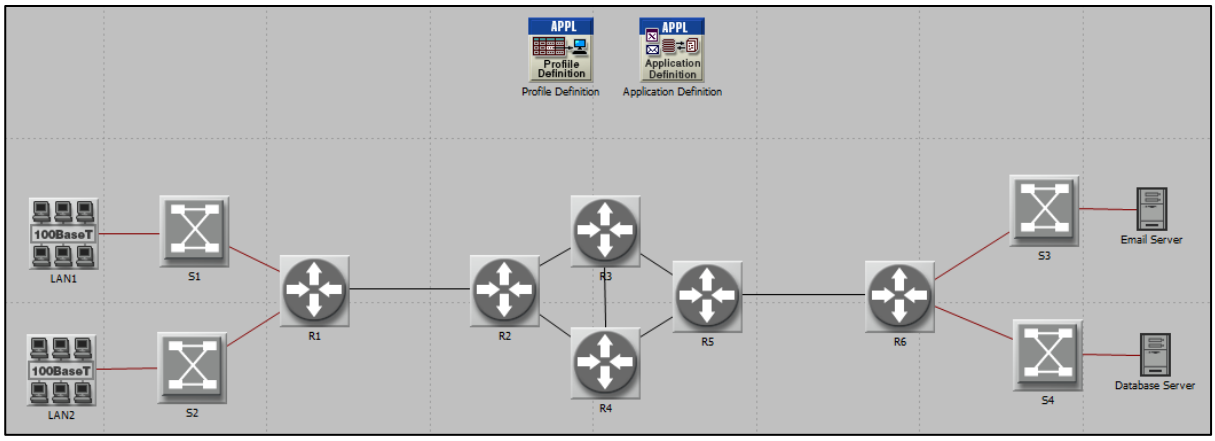

Figure 29. Network Topology

An application was chosen to be accessed (as shown at the top of the above figure). The following performance tests were then run to measure the stress on the various elements:

CPU Utilisation of the router will report, in percentage, the utilisation of the CPU resources for the various activities in a given time frame. It will also take into account the background utilisation.

Traffic dropped will be calculated by the number of IP datagrams that are dropped per second by the router.

Processing delay, calculated in seconds, the delay which is experienced by an IP datagram within the given IP layer. In other words, this shows the delay from when the packet arrives to when it leaves the IP layer. This delay includes queuing delay (to get to the head of the queue to start processing) and processing delay (based on the processing speed/forwarding rate)

6.2. Results and Discussion

The results which have been shown below are taken from router R6. They are explained with graphs as follows.

6.2.1. CPU Utilisation

The results in figure 30 show that the inefficient scenarios were for the 6to4 and manual tunnels, which utilised more than 50% resources as compared with dual stack. The most efficient scenarios were native IPv4 and IPv6 networks which utilised approximately 50% less resources as compared with the dual stack.

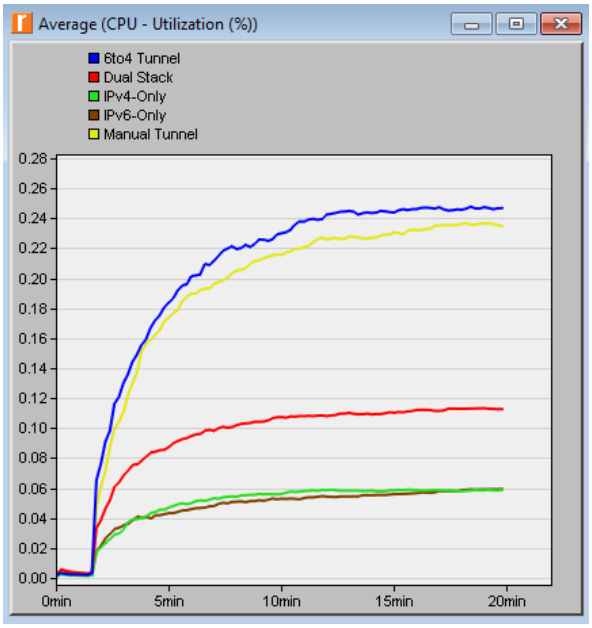

Figure 30. CPU utilization

6.2.2. Traffic Dropped

The results of this analysis in figure 31 show that dual-stack, IPv4 and IPv6 scenarios dropped a negligible number of packets. On the other hand, both the manual and 6to4 tunnel dropped a high number of packets initially. However, with the passing of time the 6to4 tunnel dropped more packets while the manual tunnel dropped fewer packets.

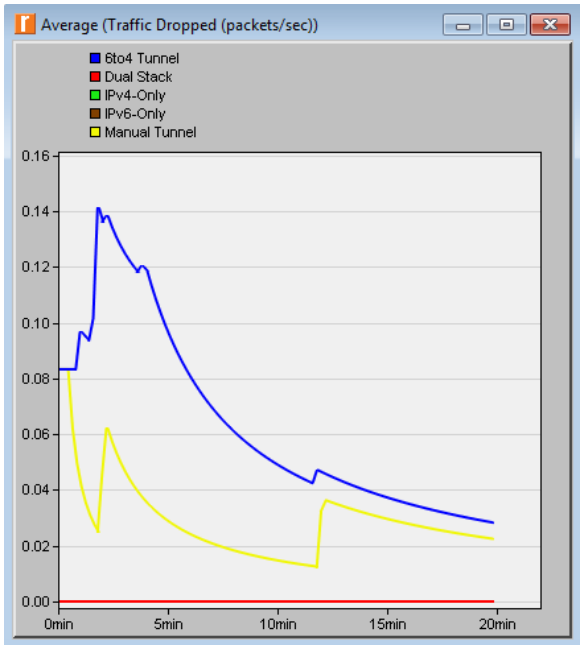

Figure 31. Average traffic dropped

6.2.3. IP Processing Delay

The results of this analysis in figure 32 are varied; however, the general trend is that all scenarios began with an increase in processing delay, with both 6to4 and manual tunnels producing the highest delay. On the other hand, the dual-stack, IPv4 and IPv6 scenarios levelled out fairly quickly, providing an average delay of 0.000020 while the 6to4 tunnel was giving a delay of 0.000021 on average. It can be seen that throughout the analysis, the 6to4 tunnel has the highest processing delay; this is because the end-point of the tunnel is not configured, as it is an automatic tunnel.

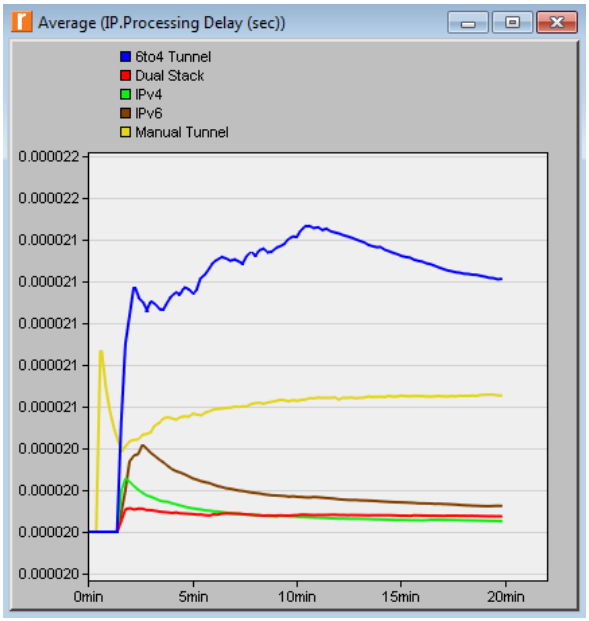

Figure 32. Average processing delay

6.3. Discussion

The simulation ran for 20 minutes. The performance analysis has shown both 6to4 and manual tunnel scenarios have been inefficient compared to others, providing the most CPU utilisation, the most number of packets dropped and the highest processing delay in all scenarios. A comparison of all the results has been shown in Table 2.

Table 2. Scenario comparison

Scenario	CPU Utilisation (seconds)	Traffic Dropped (packets/sec)	IP Processing Delay (seconds)
6to4 Tunnel	0.25	0.03	0.000021
Dual Stack	0.11	0.00	0.000020
IPv4	0.06	0.00	0.000020
IPv6	0.06	0.00	0.000020
Manual Tunnel	0.229	0.025	0.000021

7. CONCLUSION

The aim of this study was to investigate dual stack and tunnelling technologies while also looking at security risks of IPv6 and transition technologies. To investigate the two technologies, two mechanisms, dual stack and tunnelling, were broken down into their respective parts to get a deeper understanding. IPv6 transition relies on transition mechanisms to complete a successful migration. Therefore both dual stack and tunnelling mechanisms are essential elements which need further investigation. These two transition mechanisms allow for IPv4 and IPv6 devices to work in the same network in the various ways described above, however, leaves severe vulnerabilities. As with anything in networking, there are security implications which must be investigated. IPv6, dual-stack and tunnelling mechanisms have their risks. The two most common attacks which can be seen in IPv6 protocols, dual stack and tunnelling technologies are DoS and spoofing attacks; however, there are many other attacks which apply to each technology. Implementation of the dual stack and tunnel scenarios allowed us to understand the various complexities involved in each mechanism while also briefly investigating the security risks associated. With these security risks in mind, we carried out some simple attacks to simulate the ease with which one can attack the network. The performance analyses conducted clearly showed that the tunnelling mechanisms causes slight performance issues.

REFERENCES

Fatah, F.N., & Suhendra, A. (2013). Performance Measurements Analysis of Dual Stack. Proceedings of The Conference on Advances in Information Technology (pp. 100-107).

Hassan, R., & Ahmed, A. S. (2013). Avoiding Spoofing Threat in IPv6 Tunnel by Enhancing IPSec. International Journal of Advancements in Computing Technology, 5(5), 1241–1250.

Hou, H., Zhao, Q., & Ma, Y. (2010). Design and Implementation of a Solution. AIAI.

J., Hanumanthappa, & Manjaiah. D.H. (2009). IPv6 an IPv4 Threat reviews with Automatic Tunnelling and Configuration Tunnelling Considerations Transitional Model. International Journal of Computer Science and Information Security, 3(1).

Lai, G.-H. (2014). A Light-Weight Penetration Test Tool For Ipv6 Threats. IEEE. doi:10.1109/IIH-MSP.2014.19

Liu, T., Guan, X., Zheng, Q., & Qu, Y. (2009). A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks. IEEE Networks, 23(5).

Transition Mechanisms (IPv6) Part 1. (n. d.). What-when-how. Retrieved from http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-1/

Narayan, S., & Tauch, S. (2010). Network Performance Evaluation of IPv4-v6 Configured Tunnel and 6to4 Transition Mechanisms on Windows Server Operating Systems. Proceedings of the International Conference On Computer Design and Applications (pp. 435-440).

Sabir, M. R., Fahiem, M. A., & Mian, M. S. (2009). An Overview of IPv4 to IPv6 Transition and Security Issues. IEEE. doi:10.1109/CMC.2009.137

Sankaranarayanan, K., & Shalini Punithavathani, D. (2009). IPv4/IPv6 Transition Mechanisms. European Journal of Scientific Research, 34(1), 110-124.

Shah, J.L., & Parvez, J. (2014, July). An examination of next generation IP migration techniques: Constraints and evaluation. Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 776-781). IEEE.

Taib, A.M., & Budiarto, R. (2010). Securing Tunnel Endpoints for IPv6 Transition in Enterprise Networks. Proceedings of the International Conference on Science and Social Research (pp. 1114-1119). doi:10.1109/CSSR.2010.5773699

Taib, A.H.M., & Budiarto, R. (2007). Security Mechanisms for the IPv4 to IPv6 Transition. 5th Proceedings of the Student Conference on Research and Development SCOReD '07, Selangor, Malaysia, (pp. 1-6). doi: 10.1109/SCORED.2007.4451365

Thc.org. (n. d.). THC-IPV6 - Attacking The IPV6 Protocol Suite.

Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A State-of-the-Art Survey. IEEE.

Wu, Y., & Zhou, X. (2011). Research on the IPv6 Performance Analysis Based on Dual-Protocol Stack and Tunnel Transition. Proceedings of the International Conference on Computer Science & Education (pp. 1091-1093). doi:10.1109/ICCSE.2011.6028824

Xiong, W., Zhang, J.-W., & Zhang, G.-D. (2009). Application Research on IPv4/IPv6 Dual Stack Technology. Proceedings of the International Conference on Signal Processing Systems (pp. 826-828). doi:10.1109/ICSPS.2009.200

Zagar, D., & Grgic, K. (2006). IPv6 security threats and possible solutions. Proceedings of World Automation Congress WAC‘06.

Zhou, H. (2014). Strategy and Study of the Transition Technologies from IPv4 to IPv6. IEEE

Biographies:

Wael Alzaid has finished MSc in the School of Computing, Teesside University, UK. He has also done Bachelor of Engineering with Honours in Computers Networking and Communications Technology and Diploma in Computer Networks. He has research interest in computer networks, IPv6 and network security.

Biju Issac is a senior lecturer in the School of Computing, Teesside University, UK. He has done Bachelor of Engineering in Electronics and Communication Engineering (ECE), Master of Computer Applications MCA) with honours and PhD in Networking and Mobile Communications, by research. He is a Charted Engineer (CEng), and Senior Member of IEEE. His broad research interests are in Wireless Networks, Computer or Network Security, Securing Network Protocols, Mobility Management in 802.11 Networks, Intelligent Data Mining using AI, Intelligent Spam Detection, Secure Electronic Voting etc.